UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,521	08/01/2003	Kim Cameron	303187.01	4349

69316 7590 08/24/2009

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052

EXAMINER	
TIMBLIN, ROBERT M	
ART UNIT	PAPER NUMBER
2167	

NOTIFICATION DATE	DELIVERY MODE
08/24/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DBOUTON@MICROSOFT.COM
vffiling@microsoft.com
stevensp@microsoft.com

Office Action Summary	Application No.	Applicant(s)	
	10/632,521	CAMERON ET AL.	
	Examiner	Art Unit	
	ROBERT TIMBLIN	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,15-26,28-73 and 80-84* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,15-26,28-73 and 80-84* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to application 10/632,521 filed on 8/1/2003.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/8/2009 has been entered.

Response to Amendment

Claims 1-11, 15-26, 28-73, and 80-84 are pending. Claims 1, 2, 18, 19, 30, 46, 53, 60, 61, 65, 66, 80, 81, 82 have been amended, claims 27 and 85 cancelled, and, no new claims have been added in Applicant's communication filed 6/8/2009. Response to Applicant's arguments begin on page 30 of this Action.

Claim Objections

Claim 1 is objected to because it recites "on a multiple passwords". It is interpreted that this phrase should read "on multiple passwords".

Claims 28 and 29 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to

cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Specifically, claim 28 depends upon cancelled claim 27. Claim 29 depends upon claim 28 which in turn depends upon claim 27 and is objected to for the same rationale.

Claim 53 is objected to because phrases such as "for password management", "to find", "to manage", "to perform", "to display" and "to designate", "to determine", and "to collectively manage" should be positively recited as to obviate the interpretation that the recited function is *intended* to happen (i.e. suggested by "to" or "for") rather than required to happen.

Claim 56 is further objected to for the same rationale as claim 53 (i.e. stating "to display").

Claim 58 is further objected to for the same rationale as claim 53 (i.e. stating "to obtain").

Claim 59 is further objected to for the same rationale as claim 53 (i.e. stating "to perform").

Claim 61 is objected to because phrases such as "for coupling", "capable of", "to manage", "for communicating", "for searching" and "for checking" should be positively recited as to obviate the interpretation that the recited function is *intended* to happen (i.e. suggested by "capable of" "to" or "for") rather than required to happen.

Claim 63 is further objected to for the same rationale as claim 53 (i.e. stating "to change").

Claim 64 is further objected to for the same rationale as claim 61 (i.e. stating "to set").

Claim 65 is objected to because phrases such as "for persisting", "for producing", "for allowing", "to cause", "for requesting" and "to communicatively couple" should be positively recited as to obviate the interpretation that the recited function is *intended* to happen (i.e. suggested by "to" or "for") rather than required to happen.

Appropriate correction in light of the above claim objections is respectfully requested.

Claim Rejections - 35 USC § 112

The previous claim rejection under 112 2nd paragraph has been withdrawn in light of the cancellations.

35 USC § 101

The previous 35 U.S.C. 101 rejection to Claim 65 and dependents has been withdrawn. As the system now comprises computer implemented components and thus includes a computer (as supported by fig. 15 to be a hardware system) to obviate the interpretation of software per se, a statutory machine is defined.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for

patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-11, 15-18, 20, 22-26, 28-32, 35-36, 51-52, and 80-84 are rejected under 35 U.S.C. 102(e) as being disclosed by Hollingsworth (U.S. Patent 7,200,864). In the following, Hollingsworth teaches

With respect to claim 1, Hollingsworth teaches method, comprising:

outputting a user interface (300) configured to interact with an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) to perform collective password management (col. 2 line 54-57 and col. 3 line 52; i.e. universal control of passwords) for multiple user accounts (col. 5 lines 60-67; e.g. a technician's access to systems 310), each of the multiple user accounts (310) being associated with a single user (335,330 as well as col. 1 lines 36-39 and 56, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them");

receiving a selection (col. 4 line 35-40) of multiple data sources (315) connected to the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) input by the user via the user interface (300), wherein:

each of the multiple data sources (310) corresponds to a different one of said multiple user accounts (310 and 335; i.e. a user-assigned password for a system represents an account);

the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent for each of the multiple data sources configured specifically for its respective data source (col. 8 line 8-13; i.e. the adjustment of the secondary programs to allow the universal program to access and change the passwords of such

secondary programs suggests a description of an agent for the secondary program) to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (system list 310); and

for at least some of the multiple data sources (figure 3, systems A-E) a management agent for the data source is configured with credentials to perform password management for a corresponding said user account (col. 8 line 10-12);

receiving a new password (362) input by the single user (col. 1 line 56 and col. 2 line 54) via the user interface (300); and

performing an administrative password operation on a multiple passwords (col. 3 line 51-53) each associated with each one of the selected multiple data sources (310) to collectively update each said of the multiple passwords (figure 3 and col. 37-40) to the new password (362), wherein the password operation is performed using the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords).

With respect to claim 2, Hollingsworth teaches the method as recited in claim 1, further comprising:

determining an identity of the single user (col. 2 line 1; e.g. a user log in), wherein the multiple data sources are associated with (col. 7 lines 58-60) the identity (335); and

querying the identity integration system to find the multiple data sources associated with the identity (col. 4 line 26-30; e.g. a list of programs to be controlled by a user).

With respect to claim 3, Hollingsworth teaches the method as recited in claim 1, wherein the password operation comprises updating one or more passwords associated with the multiple data sources using joined objects across the multiple data sources, wherein the joined objects are stored in the identity integration system (figure 3, 315).

With respect to claim 4, Hollingsworth teaches the method as recited in claim 3, wherein some of the multiple passwords are updated to new passwords that differ from each other (335; e.g. 'monkey1' and 'kitten2').

With respect to claim 5, Hollingsworth teaches the method as recited in claim 3, wherein each of the multiple passwords is updated to the same password (335, e.g. 'monkey1').

With respect to claim 6, Hollingsworth teaches, the method as recited in claim 1, wherein the password operation comprises one of changing, setting and resetting the password (col. 3 line 51-53).

With respect to claim 7, Hollingsworth teaches the method as recited in claim 1, wherein each of the multiple data sources differ from others of the multiple data sources with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage (col. 1 line 44-50).

With respect to claim 8, Hollingsworth further teaches the method as recited in claim 1, wherein each of the multiple data sources differs in a connection to the identity integration system with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage (figure 2).

With respect to claim 9, Hollingsworth teaches the method as recited in claim 1, wherein each of the multiple data sources uses a different password management function (col. 3 line 1-5; e.g. each program having its own specific password).

With respect to claim 10, the method as recited in claim 9, wherein the identity integration system performs password management for each of the multiple data sources (col. 1 lie 36-38).

With respect to claim 11, Hollingsworth teaches the method as recited in claim 1, wherein for at least some of the multiple data sources the identity integration system stores integrated identity information to perform password management (col. 1 line 55).

With respect to claim 15, Hollingsworth teaches the method as recited in claim 1, further comprising using the identity integration system to produce a list of user accounts associated with the multiple data sources, wherein the user accounts on the list are eligible for password management (figure 3).

With respect to claim 16, Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

With respect to claim 17, Stone teaches the method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application (0077).

With respect to claim 18, Hollingsworth teaches the method as recited in claim 17, wherein the web application accepts a password credential from the single user to perform the password operation (figure 3, 366 and 362).

With respect to claim 20, Hollingsworth teaches the method as recited in claim 17, further comprising using the identity integration system to produce a list of user accounts

displayable on the website, wherein the user accounts are associated with the multiple data sources (figure 3).

With respect to claim 22, Hollingsworth teaches the method as recited in claim 17, further comprising communicatively coupling the identity integration system with the web application using an interface (figure 2).

With respect to claim 23, Hollingsworth teaches the method as recited in claim 22, wherein the interface is publicly available (col. 2 line 1-2; e.g. a user needing to log into the program describes that any user can be available to the system.

With respect to claim 24, Stone teaches he method as recited in claim 22, wherein the interface allows a web application designer to customize the web application (0021).

With respect to claim 25, Hollingsworth teaches the method as recited in claim 22, wherein the interface includes password management functions (350).

With respect to claim 26, Hollingsworth teaches the method as recited in claim 22, wherein the interface is capable of being changed for an improved version of the interface that adds more password management functions while using the same web application and the same identity integration system (col. 8 line 45-46).

With respect to claim 28, Hollingsworth teaches the method as recited in claim 27, wherein the interface is secured using a security group (col. 7 line 58-60; e.g. authorized personnel).

With respect to claim 29, Hollingsworth teaches the method as recited in claim 28, wherein the interface is secured using a security group that allows both searching for a connector object associated with a data source and setting a password for an object in the data source, wherein a connector object represents at least part of the data source in the identity integration system (col. 1 line 61-67).

With respect to claim 30, Hollingsworth teaches the method as recited in claim 1, wherein an identity of the single user associated with the multiple data sources provides a security credential for performing a password operation (coo. 2 line 1).

With respect to claim 31, Hollingsworth teaches the method as recited in claim 17, wherein the web application produces a list of accounts associated with a user (figure 3, 315).

With respect to claim 32, Hollingsworth teaches the method as recited in claim 31, wherein the web application lists only accounts eligible for password management (figure 3, 315).

With respect to claim 35 Hollingsworth teaches the method as recited in claim 17, wherein the web application checks if one of the data sources is communicating before updating

a password associated with the data source (col. 4 line 28-29; e.g. listing of the accessible programs).

With respect to claim 36 Hollingsworth teaches the method as recited in claim 35, wherein the updating comprises one of changing and setting the password (col. 3 line 51-52).

With respect to claim 51, Hollingsworth teaches the method as recited in claim 1, wherein the password operation further comprises updating passwords in both secure and non-secure data sources within the multiple data sources (col. 7 line 55-60).

With respect to claim 52, Hollingsworth teaches the method as recited in claim 1, wherein the password operation further comprises updating passwords over both secure and non-secure connections to the multiple data sources (col. 3 line 1-15).

With respect to claim 80, A computer-implemented method comprising:

retrieving a list of user accounts (310) that correspond to a single user (335,330 as well as col. 1 lines 36-39 and 55, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them") from an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) having persisted identity information (col. 1 line 55 and col. 7 line 67-col. 8 line 10; i.e. storing passwords) regarding the user accounts (310 and col. 2 line 19-21) wherein, the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling

passwords) includes a management agent (col. 8 line 10-13) for each of multiple data sources (310, systems A-E) configured specifically for its respective data source (col. 8 line 10-13) to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (310, systems A-E);

outputting a user interface (300) showing the list of user accounts (310) that correspond to the single user (335,330 as well as col. 1 lines 36-39 and 55, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them")on a display (figure 3);

allowing each account (i.e. the systems/programs in figure 3) in the list to be selected (315) using a user interface (figure 3) selection device (col. 4 line 23-25; e.g. a mouse or keyboard choosing means) operable to input selections (315) via the user interface (300) output on the display (figure 3);

allowing input of a new password (362) via the user interface selection device (col. 4 line 23-25; e.g. a mouse or keyboard choosing means); and

allowing input of a request to update old passwords (360) associated with each of the selected accounts (315, "X" marks) to the new password (365) input via the user interface (300).

With respect to claim 81, the method as recited in claim 80, further comprising allowing input of user credentials to verify an identity of the single user (366).

With respect to claim 82, One or more computer readable storage media containing instructions that are executable by a computer to perform actions, comprising:

selecting multiple data sources (315, 310) connected to an identity integration system col. 2 line 54-56; e.g. universal access program for controlling passwords);

receiving a new password (362) input by a single user to cause the new password (362) to be associated with each of the selected multiple data sources (315); and

using the identity integration system col. 2 line 54-56; e.g. universal access program for controlling passwords) to collectively update (col. 2 line 54-57 and col. 3 line 52) a password associated with each of the selected multiple data sources (335) to the new password input by the single user (362).

With respect to claim 83, the one or more computer readable storage media as recited in claim 82, wherein at least some of the multiple data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (figure 1 and col. 5 line 20-25; e.g. the universal system may communicate with various computer systems).

With respect to claim 84, the one or more computer readable storage media as recited in claim 82, wherein the identity integration system accomplishes a password update on each of the data sources regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (col. 2 line 51-55).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 19, 33, 34, 37-50, 53-60, 61-69, and 71-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollingsworth in view of Stone et al. ('Stone' hereafter, U.S. Patent Application 2007/0094392).

With respect to claim 19, Hollingsworth does not expressly teach wherein the web application verifies an identity of the single user by asking the user questions, wherein if answers provided by the user are correct then the web application performs the password operation using the identity of a privileged user account.

Stone, however, teaches wherein the web application verifies an identity of a user by asking the user questions (figure 20, s104), wherein if answers provided by the user are correct (5106) then the web application performs the password operation using the identity of a privileged user account (figure 20).

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the above limitations would further enable Hollingsworth's system to further verify a user.

With respect to claim 33 Hollingsworth does not appear to teach the method as recited in claim 17, wherein the web application adopts a web application behavior based on a configuration setting.

Stone, however, teaches the method as recited in claim 17, wherein the web application adopts a web application behavior based on a configuration setting (0042, (3)) for user preferences.

Accordingly, in the same field of endeavor, (i.e. password), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a user profile for the benefit of improved security by identifying a user, identifying permissions and keeping track of a users associated resources.

With respect to claim 34, Hollingsworth and Stone further teach the method as recited in claim 33, wherein the 15 configuration setting is stored in a configuration file (Stone, 0042; e.g. a profile of a user).

With respect to claim 37, Hollingsworth does not appear to teach checking if a connection to one of the data sources is secure before updating a password associated with the data source.

Stone, however, teaches the method as recited in claim 17, wherein the web application checks if a connection to one of the data sources is secure before updating a password associated with the data source (0022, 0048) for supporting a secure transmission.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have provided a secure information transmission means for the benefit of added security while managing passwords.

With respect to claim 38, Hollingsworth teaches the method as recited in claim 37, wherein the updating comprises one of changing and setting the password (col. 3 line 51-52).

With respect to claim 39, Hollingsworth does not appear to teach displaying a status for the password operation.

Stone, however, teaches the method as recited in claim 1, further comprising displaying a status for the password operation (0106, 0124) for acknowledging an update.

In the same field of endeavor, (i.e. password management) it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stones teaching would have given a user of Hollingsworth a notification that an password change was acknowledged for assurance of a password operation.

With respect to claim 40, Hollingsworth and Stone further teach the method as recited in claim 39, further comprising displaying the status on a webpage (Stone, 0077).

With respect to claim 41, Hollingsworth does not appear to teach auditing the password operation.

Stone, however, teaches the method as recited in claim 1, further comprising auditing the password operation (0028; i.e. success/error logs).

In the same field of endeavor, (i.e. password management) it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stones teaching would have given Hollingsworth the ability to detect invalid users for purposes of mitigating intrusion.

With respect to claim 42, Hollingsworth and Stone further teach the method as recited in claim 41, further comprising maintaining a password management history for the password operation (Stone, 0028; i.e. archiving the logs).

With respect to claim 43, Hollingsworth and Stone further teach the method as recited in claim 42, further comprising keeping the password management history in a connector space object, wherein the connector space object is included in the identity integration system (Stone, 0025).

With respect to claim 44, Hollingsworth and Stone further teach the method as recited in claim 42, wherein the password management history includes a tracking identifier to an audit record of the password operation (Stone, 0028).

With respect to claim 45, Hollingsworth and Stone further teach the method as recited in claim 41, further comprising maintaining a repository of audit records for password operations performed using the identity integration system (Stone, 0082, drawing reference 42).

With respect to claim 46, Stone teaches the method as recited in claim 45, wherein an audit 10 record for a password operation includes at least one of an identifier of a single user associated with the password operation, a tracking identifier to a web application initiating the password operation, a tracking identifier to a connector object associated with the password operation, a tracking identifier to a management agent associated with the password operation, a password operation identifier, a password operation status, a date, and a time (0028, 0082).

With respect to claim 47, Stone teaches the method as recited in claim 1, further comprising associating custom logic (24, 0028, 0124) with a password operation, wherein the custom logic is executed after the password operation is performed (0052, 0074) for providing operations concerning a password operation.

Accordingly, in the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone's logic would have provided password operation assurance and credibility information for a more secure accessing system.

With respect to claim 48, Stone teaches the method as recited in claim 47, wherein the custom logic sends an email (0106 and 0085).

With respect to claim 49, Stone teaches the method as recited in claim 47, wherein the custom logic logs password management activity (0028).

With respect to claim 50, Stone teaches the method as recited in claim 47, wherein the custom logic performs a password operation on a subsequent data source not connected to the identity integration system (figure 5).

With respect to claim 53, Hollingsworth teaches An apparatus comprising:

a processor (col. 4 line 20-25); and

a user identifier to find user identity information (col. 2 line 1-3 e.g. a login) in an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), that corresponds to a single user (335,330 as well as col. 1 lines 36-39 and 55; e.g. a user can change passwords, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them") wherein:

the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent (col. 8 line 10-13; e.g. secondary programs having their own passwords for access) for each of multiple data sources to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access

program for controlling passwords), systems marked by 'X') and each respective data source (315); and

identity information query logic to search information in the identity integration system for accounts associated with the user (col. 4 line 25-30 and figure 3; i.e. listing the systems accessible by a user);

an account lister to display (300) the accounts associated with the user (figure 3, 310);

an account selector (col. 2 line 25-27) to designate at least some of the displayed accounts (300, fig. 3) for password management (300);

a password inputter (362) to determine a new password (365) input by the single user to associate with each designated accounts (figure 3, systems marked by 'X'); and

a password manager (col. 1 line 51; e.g. a control program to change passwords) to collectively manage passwords (col. 4 line 37-40) for the designated accounts (figure 3) that correspond to the single user (335,330 as well as col. 1 lines 36-39 and 55, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them"), systems marked by 'X') by requesting an update of a password associated with each designated figure 3, systems marked by 'X') account to the new password (365), responsive to the user input (col. 4 line 30-40).

Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the

teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

Hollingsworth further does not expressly disclose for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source.

Stone, however, teaches for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code (e.g. and XML file), from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source (drawing reference 24 and paragraphs 0038-0042) as a file or data structure composed by a system administrator to modify user attributes including user access data.

In the same field of endeavor, (i.e. user access privileges), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth custom logic in the form of a file from an administrator for customizing the password management process in controlling various and multiple programs. Further, the custom logic as provided by Stone would have given the personnel of Hollingsworth's system more control over editing passwords for the multiple programs (as shown by Hollingsworth, col. 7 line 57-60).

With respect to claim 54, Hollingsworth teaches the apparatus as recited in claim 53, wherein the identity integration system connects with diverse data sources, each data source having a different function for using password security (col. 3 line 1-5; e.g. each program having its own specific password).

With respect to claim 55, Hollingsworth and Stone further teach the apparatus as recited in claim 53, further comprising an account status display to show selected accounts and a connection status of each account (Stone, 0091).

With respect to claim 56, Hollingsworth and Stone further teach the apparatus as recited in claim 53, further comprising a password management status display to display a password management operation status for each account (Stone, 0106, 0124).

With respect to claim 57, Hollingsworth and Stone further teach the apparatus as recited in claim 53, further comprising a status checker to verify connectivity and security of a connection between an account and the identity integration system (Stone, 0022, 0048).

With respect to claim 58 Hollingsworth and Stone further teach the apparatus as recited in claim 53, further comprising a configuration reader to obtain behavior settings for the web application (Stone, 0042).

With respect to claim 59, Hollingsworth and Stone further teach teaches the apparatus as recited in claim 53, further comprising a custom logic executor to perform custom logic associated with a password management operation (Stone, 0024, receiver 28).

With respect to claim 60, Hollingsworth teaches the apparatus as recited in claim 53, wherein the account lister lists only accounts eligible for password management (figure 3 and col. 4 line 26-30) and does not list accounts that are not eligible for password management (col. 7 lines 58-60; e.g. the personnel may only access, edit, and change the passwords of those programs that have already been preauthorized for them and further fig. 3 listing the programs associated with the control system).

With respect to claim 61, Hollingsworth teaches an apparatus comprising a processor coupled to memory, the memory storing one or more modules executable via the processor to implement:

an interface for coupling an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords);

logic for communicating with the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), wherein: the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) is capable of collectively updating a password (col. 4 line 37-40) on multiple data sources (310) that use various functions of password updating (col. 3 line 1-5) responsive to input of a single new password (365) by a single user (335,330 as well as col. 1 lines 36-39 and 55, and col. 7 lines 58-

60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them");

each said data source (systems 310)includes a user account (310; systems A-E) that corresponds to the single user (335,330 as well as col. 1 lines 36-39 and 55, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them");

the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent (col. 8 line 10-13) for each of the multiple data sources (315) to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (315); for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management (col. 8 line 10-12); and

logic for checking a connection status between the identity integration system and a data source (col. 4 line 26-30; i.e. listing accessible programs).

Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit

would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

With respect to claim 62, Hollingsworth and Stone further teach the apparatus as recited in claim 61, further comprising logic for checking security of a connection between the identity integration system and a data source (0022 and 0048).

With respect to claim 63, Hollingsworth teaches the apparatus as recited in claim 61, further comprising logic to change a password associated with the data source (col. 3 line 50-53).

With respect to claim 64, Hollingsworth teaches the apparatus as recited in claim 61, further comprising logic to set a password associated with the data source (col. 3 line 51).

With respect to claim 65, Hollingsworth teaches A password management system, comprising:

an identity integration system implemented by a computer (col. 2 line 54-56; e.g. universal access program for controlling passwords) having a metaverse space for persisting integrated identity information regarding accounts associated with a single user (figure 3 and col. 7 line 65-col. 8 line 5), and a connector space for persisting information representing multiple data sources connectable to the identity integration system (335), the accounts each corresponding to one of the multiple data sources and having associated manageable passwords (figure 3);

a web application implemented by the computer for producing a list of the accounts (310) from the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), for allowing selection of at least some of the accounts (315), configured for input of a new password (362) to cause the new password to be associated with each of the selected accounts (col.3 line 51), and for requesting the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) to collectively update passwords (col. 4 line 35-40) on each of the selected accounts to the input new password (362); and

an interface implemented by a computer to communicatively couple the identity integration system with the web application (figure 2).

Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

With respect to claim 66, Hollinger teaches the password management system as recited in claim 65, wherein the password management web application verifies one of an identity and a credential of the single user (col. 2 line 1 and 366).

With respect to claim 67, Hollingsworth and Stone further teach the password management system as recited in claim 65, wherein the web application generates a webpage that displays accounts and a status of a password management operation for each account displayed (0106, 0124).

With respect to claim 68, Hollingsworth teaches the password management system as recited in claim 65, wherein the web application operates in a security context (col. 7 line 57-60).

With respect to claim 69, Hollingsworth teaches the password management system as recited in claim 68, wherein the security context is an application pool identity (col. 7 line 57-60; e.g. authorized personnel).

With respect to claim 71, Hollingsworth and Stone further teach the password management system as recited in claim 65, wherein the identity integration system stores a password management operation history for each account (Stone, 0028; i.e. archiving the login attempts).

With respect to claim 72, Hollinger teaches the password management system as recited in claim 65, wherein the identity integration system communicates with diverse accounts, each account having a different mechanism for administering a password associated with the account (figure 2; i.e. communicating with multiple programs).

With respect to claim 73, Hollingsworth and Stone further teach the password management system as recited in claim 72, wherein the identity integration system does not natively communicate with at least some of the diverse accounts (Stone, 0019 and 0045-0046).

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hollingsworth as applied to claim 1 above in view of Bush et al. ('Bush' hereafter) (U.S. Patent Application 2002/0083012).

With respect to claim 21, the Hollingsworth fails to teach a help desk to at least assist in the performing a password operation.

Bush, however, teaches a help desk to at least assist in the performing a password operation (0024, i.e. sending a password by telephone to the user) for assisting in new user registration.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Bush's system would have given Hollinger and Stone's system a more user friendly and efficient method of helping a user to establish an account.

Claim 70 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hollingsworth and Stone as applied to claim 65 above in view of Bush.

With respect to claim 70, the Hollingsworth and Stone fails to teach the password management system as recited in claim 69, further comprising a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application.

Bush, however, teaches a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application (0024, and 0039) for assisting in new user registration.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Bush's system would have given Hollinger and Stone's system a more user friendly and efficient method of helping a user to establish an account.

Response to Arguments

Applicant's arguments filed in the reply dated 6/8/2009 ("reply") have been fully considered but they are not persuasive. Examiner respectfully traverses Applicant's remarks in the following:

In the independent claims, Applicant has amended to clarify that accounts are associated with a single user and thus submits the claims to be allowable. Examiner respectfully disagrees.

While appreciating the further clarity given to the claims, Examiner respectfully submits that the claims as amended do not distinguish over the prior art (namely, Hollingsworth). Specifically, a review and reconsideration of Hollingsworth reveals that "multiple user accounts being associated with a single user" is taught.

Specifically, Hollingsworth teaches the multiple user accounts (310) being associated with a single user (335,330 as well as col. 1 lines 36-39 and 56, and col. 7 lines 58-60; e.g. …"thus personnel may only access, edit and change the passwords of those programs that have already been preauthorized for them")

As such, Hollingsworth teaches that *a* user is provided with a single universal system of controlling multiple passwords for multiple programs (e.g. accounts) in col. 1 lines 36-37. Hollingsworth also states their program to enable *a* user to instantly change all passwords of all programs by a few simple operations (e.g. col. 1 lines 56-58). Hollingsworth further teaches a [given] personnel may also access, edit, and change the passwords of those programs that have already been preauthorized for them (col. 7 lines 45-60). As such, a given personnel (e.g. a technician, col. 6 lines 28-30 or *the* technician col. 5 line 61) is preauthorized to access and edit programs specific to them. Because *a* user or *a/the* technician (i.e. 'single') is preauthorized (e.g. 'associated') with the programs, and is further able to manage those programs associated to them, Examiner respectfully submits the amended limitation is taught.

Conclusion

U.S. Patent Application 2004/0230914 filed by Arend et el. The subject matter therein pertains to the pending claims (i.e. finding associated accounts to a single user; e.g. 0034,0036).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ROBERT TIMBLIN whose telephone number is (571)272-5627. The examiner can normally be reached on M-Th 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ROBERT TIMBLIN/

Examiner, Art Unit 2167